providing the PRC End-User Certificate Number to BIS, you must identify the transaction in the post shipment report to which that PRC End-User Certificate Number applies.

(C) *Mailing address.* A copy of the post-shipment report[s] required under paragraph (b)(3)(iv)(A) of this section shall be delivered to one of the following addresses. Note that BIS will not accept reports sent C.O.D.

(*1*) For deliveries by U.S. postal service: U.S. Department of Commerce, Bureau of Industry and Security, P.O. Box 273, Washington, D.C. 20044, Attn: Office of Enforcement Analysis HPC Team, Room 4065.

(*2*) For courier deliveries: U.S. Department of Commerce, Office of Enforcement Analysis HPC Team, 14th Street and Constitution Ave., NW, Room 4065, Washington, DC 20230.

(4) *Computer Tier 4*—(i) *License requirement.* A license is required to export or reexport any items covered by this section to a country in Country Tier 4.

(ii) *Licensing policy.* The licensing policies for countries in Computer Tier 4 are the same as described in the following EAR sections: for Sudan see §742.10(b); for Syria see §742.9(b); for Cuba see §746.2; for Iran see §746.7; for Libya see §746.4; and for North Korea see §742.19(b).

(c) *Contract sanctity.* Contract sanctity provisions are not available for license applications involving exports and reexports of high performance computers.

(d) *High performance computer regime.* The United States and Japan participate in a high performance computer regime. The regime provides uniform and effective safeguards to protect high performance computers from unauthorized destinations, end-users and end-uses.

[61 FR 12786, Mar. 25, 1996, as amended at 61 FR 64283, Dec. 4, 1996; 63 FR 2458, Jan. 15, 1998; 63 FR 5451, Feb. 3, 1998; 63 FR 63143, Nov. 12, 1998; 63 FR 64324, Nov. 19, 1998; 64 FR 2431, Jan. 14, 1999; 64 FR 42012, Aug. 3, 1999; 65 FR 12922, Mar. 10, 2000; 65 FR 38151, June 19, 2000; 65 FR 60855, Oct. 13, 2000; 66 FR 5446, Jan. 19, 2001; 67 FR 10615, 10610, Mar. 8, 2002; 67 FR 13567, Mar. 25, 2002; 69 FR 46076, July 30, 2004]

§ 742.13 Communications intercepting devices.

(a) *License requirement.* (1) As set forth in ECCN 5A980, a license is required for the export or reexport to any destination, including Canada, of any electronic, mechanical, or other device primarily useful for surreptitious interception of wire or oral communications. This control implements a provision of the Omnibus Crime Control and Safe Streets Act of 1968 (Public Law 90–361). This license requirement is not reflected on the Country Chart (Supplement No. 1 to part 738 of the EAR).

(2) Communications intercepting devices are electronic, mechanical, or other devices that can be used for interception of wire or oral communications if their design renders them primarily useful for surreptitious listening even though they may also have innocent uses. A device is not restricted merely because it is small or may be adapted to wiretapping or eavesdropping. Some examples of devices to which these restrictions apply are: the martini olive transmitter; the infinity transmitter; the spike mike; and the disguised microphone appearing as a wristwatch, cufflink, or cigarette pack; etc. The restrictions do not apply to devices such as the parabolic microphone or other directional microphones ordinarily used by broadcasters at sports events, since these devices are not primarily useful for surreptitious listening.

(b) *Licensing policy.* (1) License applications will generally be approved for:

(i) A provider of wire or electronic communication services or an officer, agent, or employee of, or person under contract with, such a provider in the normal course of the business of providing that wire or electronic communication service; and

(ii) Officers, agents, or employees of, or person under contract with the United States, one of the 50 States, or a political subdivision thereof, when engaged in the normal course of government activities.

(2) Other applications will generally be denied.

(c) *Contract sanctity.* Contract sanctity provisions are not available for license applications involving exports

and reexports of communications interception devices.

(d) *U.S. controls.* Controls on this equipment are maintained by the United States government in accordance with the Omnibus Crime Control and Safe Streets Act of 1968.

§ 742.14 Significant items: hot section technology for the development, production or overhaul of commercial aircraft engines, components, and systems.

(a) *License requirement.* Licenses are required for all destinations, except Canada, for ECCNs having an ''SI'' under the ''Reason for Control'' paragraph. These items include hot section technology for the development, production or overhaul of commercial aircraft engines controlled under ECCN 9E003.a.1. through a.12., .f, and related controls.

(b) *Licensing policy.* Pursuant to section 6 of the Export Administration Act of 1979, as amended, foreign policy controls apply to technology required for the development, production or overhaul of commercial aircraft engines controlled by ECCN 9E003.a.1. through a.12, .f, and related controls. These controls supplement the national security controls that apply to these items. Applications for export and reexport to all destinations will be reviewed on a case-by-case basis to determine whether the export or reexport is consistent with U.S. national security and foreign policy interests. The following factors are among those that will be considered to determine what action will be taken on license applications:

(1) The country of destination;

(2) The ultimate end-user(s);

(3) The technology involved;

(4) The specific nature of the end-use(s); and

(5) The types of assurance against unauthorized use or diversion that are given in a particular case.

(c) *Contract sanctity.* Contract sanctity provisions are not available for license applications reviewed under this § 742.14.

(d) [Reserved]

[64 FR 13339, Mar. 18, 1999]

§ 742.15 Encryption items.

Encryption items can be used to maintain the secrecy of information, and thereby may be used by persons abroad to harm U.S. national security, foreign policy and law enforcement interests. The United States has a critical interest in ensuring that important and sensitive information of the public and private sector is protected. Consistent with our international obligations as a member of the Wassenaar Arrangement, the United States has a responsibility to maintain control over the export and reexport of encryption items. As the President indicated in Executive Order 13026 and in his Memorandum of November 15, 1996, exports and reexports of encryption software, like exports and reexports of encryption hardware, are controlled because of this functional capacity to encrypt information on a computer system, and not because of any informational or theoretical value that such software may reflect, contain, or represent, or that its export or reexport may convey to others abroad. For this reason, export controls on encryption software are distinguished from controls on other software regulated under the EAR.

(a) *Licensing requirements and policy—*(1) *Encryption items controlled under ECCN 5A002, 5D002, or 5E002.* (i) *Licensing requirements.* A license is required to export or reexport encryption items (''EI'') controlled under ECCN 5A002, 5D002 or 5E002 to all destinations, except Canada. Refer to part 740 of the EAR, for license exceptions that apply to certain encryption items, and to § 772.1 of the EAR for definitions of encryption items and terms. Exporters must submit applications to obtain authorization under a license or an Encryption Licensing Arrangement for exports and reexports of encryption items that are not eligible for a license exception.

(ii) *Licensing policy.* Applications will be reviewed on a case-by-case basis by BIS, in conjunction with other agencies, to determine whether the export or reexport is consistent with U.S. national security and foreign policy interests. Exports of encryption items to governments, or Internet and telecommunications service providers for